## ABSTRACT

Prior zero-knowledge protocols are used for exchanging secret keys, but not for comparing documents. The present invention provides a method of zero-knowledge document comparison between mutually distrustful parties by having each party exchange a set of random data and a shared hash function, applying the hash function to concatenations of the document and the sets of random data, and comparing the hashes.